enterprise europe network

Fiche pratique :

Règlement européen relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD)

Mme Catherine Jamon Servel, Conseil juridique européen

c.jamon@lyon-metropole.cci.fr

Mise à jour janvier 2022

een.ec.europa.eu

AUVERGNE-RHÔNE-ALPES

CCI LYON MÉTROPOLE Saint-Etienne Roanne

enterprise europe network Business Support on Your Doorstep

Le RGPD

(Règlement européen relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données)

Fiche initialement réalisée par Me Catherine CHABERT, Avocate et mise à jour par le réseau Enterprise Europe Network/ CCI LYON METROPOLE Saint Etienne Roanne.

INTRODUCTION

Après plusieurs années d'attente, le Règlement européen relatif à la protection des données à caractère personnel a été adopté le 27 avril 2016 et est entré en vigueur le 25 mai 2018.

Cette entrée en vigueur différée a permis aux organismes concernés de se mettre en conformité avec cette nouvelle réglementation.

L'objectif consiste à « assurer un niveau cohérent et élevé de protection des personnes physiques et lever les obstacles aux flux de données au sein de l'Union Européenne ».

La réglementation existante va désormais s'appliquer à toutes les organisations (entreprises privées comme organismes publics) disposant d'un établissement sur le territoire de l'Union Européenne, qu'elles effectuent le traitement de données à caractère personnel sur le territoire européen ou non.

Auparavant, seules les organisations qui effectuaient le traitement sur le territoire européen étaient concernées.

Le champ d'application de la réglementation est donc sensiblement élargi. Cela est d'autant plus vrai que la qualification « d'établissement » ne concerne pas uniquement les entreprises immatriculées dans un Etat membre. Il suffit que l'établissement même non immatriculé exerce une activité réelle et effective au moyen d'une installation stable en lien avec le traitement de données à caractère personnel (cf. CJUE, 1er octobre 2015 n° C-230/14) pour que les dispositions du Règlement s'appliquent.

D'application directe, le Règlement s'applique de manière uniforme et immédiate dans l'ensemble des Etats membres de l'Union Européenne sans qu'il soit besoin de le transposer en droit national.

Par ailleurs, le Règlement prévoit que chaque Etat membre dispose d'une marge de manœuvre pour adapter certaines dispositions à leur droit national.

S'agissant de la mise en conformité du droit français au Règlement, le Gouvernement a choisi d'adapter le cadre juridique existant en matière de collecte et d'utilisation des données personnelles sur le territoire français.

Ainsi, la loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles a apporté des modifications à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

De plus, la loi française complète certains points en prévoyant notamment l'extension des missions de régulation de la Commission Nationale de l'Informatique et des Libertés (CNIL) et apporte des précisions quant au traitement de certaines données sensibles (ex : données liées à aux condamnations pénales ou aux infractions ; données de santé…).

SYNTHESE

Ce Règlement révolutionne le fonctionnement existant jusqu'alors, **puisqu'il supprime les déclarations préalables** ; en revanche il responsabilise les organisations quant aux données qu'elles traitent.
On passe ainsi d'un régime a priori (déclaration ou autorisation préalable) à un régime d'autorégulation et de contrôle a posteriori.

Accountability : première illustration de ce changement de philosophie : le principe dit d'accountability en vertu duquel le responsable du traitement a l'obligation de mettre en œuvre des mécanismes et des procédures permettant de démontrer le respect des règles relatives à la protection des données.

En d'autres termes, le responsable du traitement n'a plus l'obligation de soumettre le traitement envisagé au contrôle préalable de la CNIL mais doit en revanche être en mesure de démontrer que le/les traitement(s) qu'il met en œuvre sont conformes au Règlement, et ce à première demande.

Privacy by design : concept développé à l'initiative de la préposée à la protection des données de l'Etat d'Ontario au Canada, Ann Cavoukian, (cf. Operationalizing Privacy by Design : A Guide to Implementing Strong Privacy Practices, Toronto 2012). L'approche « Privacy by design » constitue une seconde illustration du changement de philosophie opéré par le Règlement européen en matière de protection des données personnelles.

Cette approche vise à mettre la protection de la vie privée au centre des préoccupations du responsable du traitement en lui imposant de développer des produits et/ou des services en prenant en compte dès leur conception et tout au long de leur cycle de vie les aspects liés à la protection des données à caractère personnel afin de permettre le plus haut niveau de protection possible.

Registre : L'article 30 du règlement RGPD dispose *« Chaque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement effectuées sous leur responsabilité. »*

La tenue de ce registre est obligatoire pour les entreprises de plus de 250 salariés, et pour les entreprises de moins de 250 salariés, lorsque les traitements de données personnelles peuvent présenter un risque pour les droits et libertés des personnes concernées ou pour les entreprises dont les traitements ne sont pas occasionnels ou portent sur une catégorie de données particulières (Article 30 §5).
Le 2 décembre 2019, la Commission nationale de l'informatique et des libertés (CNIL) a publié à destination des personnes concernées par la conformité RGPD son registre des traitements.

Ce registre contient la documentation permettant aux responsables et sous-traitants de gérer et de prouver leur conformité au RGPD – Règlement n°2016/679.

Ce document contient des explications et peut servir à titre d'exemple.

https://www.cnil.fr/fr/la-cnil-publie-son-registre-rgpd
https://www.cnil.fr/sites/default/files/atoms/files/registre-rgpd-cnil_dec-2020.pdf

La CNIL fait une interprétation large de la notion de traitement non occasionnel et semble considérer que les traitements courants réalisés par les entreprises doivent être considérés comme non occasionnels. Pour ces entreprises, la tenue du registre sera obligatoire uniquement s'agissant de ces traitements non occasionnels.
Ainsi, la prudence nous conduit à considérer que toute entreprise doit se soumettre à la tenue d'un registre.
L'article 30 liste les informations devant figurer dans ce registre. La CNIL a repris ces informations sur son site et y a publié des modèles de registre : https://www.cnil.fr/fr/cartographier-vos-traitements-de-donnees-personnelles

Etudes d'impact relatives à la vie privée : lorsqu'un traitement de données est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement doit effectuer, préalablement à la mise en œuvre du traitement, une analyse de l'impact de ce dernier sur la protection des données à caractère personnel.

Le Règlement prévoit la publication d'une liste des traitements et opérations concernés par une telle analyse dans chaque Etat par les autorités de contrôle compétentes (en France, il s'agit de la CNIL).

Renforcement de l'obligation de sécurité : en parallèle des autres obligations mises à sa charge, le responsable du traitement voit également son obligation de sécurisation des traitements renforcée.
En effet, chaque responsable de traitement doit mettre en œuvre *« les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté »* (article 32).

Délégué à la Protection des Données : le responsable du traitement et le sous-traitant doivent obligatoirement désigner un Délégué à la Protection des Données (DPD) dans les cas suivants :

- Le traitement est effectué par une autorité ou un organisme public ;
- Les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui exigent un suivi régulier et systématique à grande échelle des personnes concernées ;
- Les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de données sensibles ou relatives à des condamnations pénales et à des infractions.

En dehors de ces cas, le responsable du traitement et le sous-traitant restent libres de désigner ou non un DPD.

Sous-traitance : le Règlement va au-delà de ce que prévoit l'article 35 de la loi « Informatique Libertés » qui dispose que le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité, en imposant au responsable du traitement qui choisit de faire appel à un sous-traitant **de vérifier** que ce dernier présente *« **des garanties suffisantes** quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée »* (article 28).

Dans ce contexte, il appartient au responsable du traitement de s'enquérir des pratiques et des politiques du sous-traitant en matière de protection des données à caractère personnel.

Le responsable du traitement et le sous-traitant doivent, de surcroît, être liés par un contrat **écrit** dont le Règlement liste de manière non exhaustive le contenu.

Transfert de données : le responsable du traitement et/ou les sous–traitants ne peuvent transférer des données hors UE que s'ils encadrent ces transferts avec des outils assurant un niveau de protection suffisant et approprié des personnes.

Ainsi, et hormis les transferts fondés sur une décision d'adéquation de la Commission Européenne, les responsables de traitement et les sous-traitants peuvent mettre en place :

- Des règles d'entreprises contraignantes (BCR) ;
- Des clauses contractuelles types approuvées par la Commission Européenne ;
- Des clauses contractuelles adoptées par une autorité et approuvées par la Commission européenne (exemple : privacy shield)

Par ailleurs, les données transférées hors Union restent soumises au droit de l'Union non seulement pour leur transfert, mais aussi pour tout traitement et transfert ultérieur.

Droit des personnes : les citoyens peuvent davantage contrôler leurs données personnelles.

Dans cet esprit, les sanctions sont renforcées : le responsable du traitement ainsi que le sous-traitant sont directement responsables devant les personnes concernées du respect des dispositions du Règlement.

Ainsi, en cas de violation, toute personne peut au choix introduire une réclamation devant l'autorité de contrôle compétente ou saisir directement une juridiction pour solliciter la réparation du dommage qu'elle a subi du fait de cette violation.

La violation du Règlement par le responsable du traitement ou le sous-traitant peut également donner lieu à une action de groupe.

Le responsable du traitement et le sous-traitant peuvent faire l'objet de sanctions administratives importantes en cas de méconnaissance des dispositions du Règlement.

TEXTE ET CONTENU

1) Rappel de la terminologie et des principes applicables

Le Règlement n'apporte pas de grands changements concernant les notions clés de la matière ; dont les définitions restent les mêmes :

- **Données à caractère personnel** = toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée») ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

- **Traitement** = toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

- **Responsable du traitement** = la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés

par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.

- **Sous-traitant** = la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

De même, les concepts de base de la protection des données personnelles demeurent inchangés.

Ainsi, pour être conforme à la réglementation, le responsable du traitement doit toujours faire en sorte que le traitement mis en œuvre respecte les principes suivants :

- Le traitement doit être licite, loyal et transparent au regard de la personne concernée ;
- Le traitement doit avoir une finalité déterminée, explicite et légitime ;
- Les données traitées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ;
- Les données traitées doivent être exactes et, si nécessaire, tenues à jour ; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder ;
- Les données traitées doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ;
- Les données doivent être traitées de façon à garantir une sécurité appropriée, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées

En outre, le traitement envisagé n'est licite que dans l'un des cas suivants :

- La personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ;
- Le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;
- Le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;
- Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;
- Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;
- Le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits

fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.

2) Obligations du responsable du traitement

a) Accountability

Pour se conformer à cette nouvelle obligation, les responsables de traitement doivent mettre en place des procédures et des politiques internes dédiées à la protection des données personnelles.
A cet égard, le G29 (groupe de « CNIL » européennes, aujourd'hui Comité Européen de la Protection des Données « CEPD ») a donné quelques exemples des mesures à prendre :

- La mise en place de procédures internes permettant de garantir le respect des principes de protection des données (notamment lors de la création ou la modification d'un traitement),
- L'inventaire des traitements,
- La répartition des rôles et responsabilités,
- La sensibilisation et la formation du personnel,
- La désignation d'un délégué à la protection des données,
- La vérification de l'efficacité des mesures (contrôles, audits),
- La transparence sur les politiques de confidentialité et la gestion interne des plaintes.

Le Règlement vise également l'application :

- d'un code de conduite ;
- d'un mécanisme de certification approuvé.

Naturellement, comme dans tout processus d'amélioration continue, ces **mesures doivent être régulièrement réexaminées et actualisées** si nécessaire.
Il convient enfin de noter que le seul fait de ne pas fournir les éléments attestant de la conformité du/des traitement(s) concerné(s) est susceptible d'entrainer une sanction, indépendamment de l'existence ou non d'une violation des données.

b) Privacy by design

En pratique, le responsable du traitement doit appliquer des mesures techniques et organisationnelles appropriées pour garantir que par défaut, seules sont traitées les données à caractère personnel nécessaires à la finalité du traitement.

Afin d'évaluer les mesures à mettre en œuvre, le responsable du traitement peut s'appuyer sur différents critères :

- L'état des connaissances ;

- Les coûts de mise en œuvre ;
- La nature, la portée, le contexte et la finalité du traitement ;
- Les risques que représente le traitement pour les droits et libertés des personnes concernées.

Le Règlement conseille notamment deux types de mesures :

- La pseudonymisation des données qui permet de ne plus pouvoir associer des données à une personne physique déterminée sans avoir recours à des informations supplémentaires
- La minimisation des données qui permet de ne traiter que des données adéquates, pertinentes et limitées à la finalité du traitement.

c) Etudes d'impact relatives à la vie privée

Lorsqu'un traitement de données est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement doit effectuer**, préalablement à la mise en œuvre du traitement**, une analyse de l'impact de ce dernier sur la protection des données à caractère personnel.

Une étude d'impact s'impose notamment dans les cas suivants :

- Traitement de profilage sur la base duquel sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ;
- Traitement à grande échelle de données sensibles, ou de données relatives à des condamnations pénales et à des infractions ;
- Surveillance systématique à grande échelle d'une zone accessible au public.

Une liste plus exhaustive des traitements et opérations concernés doit être publiée dans chaque Etat par les autorités de contrôle compétentes (en France, il s'agit de la CNIL).
Une étude d'impact repose sur deux piliers :

- Les principes et droits fondamentaux, « non négociables », fixés par le Règlement, lesquels ne peuvent faire l'objet d'aucune modulation ;
- La gestion des risques sur la vie privée des personnes concernées, qui permet de déterminer les mesures appropriées pour protéger les données personnelles.

L'étude d'impact comprend au moins quatre étapes :

- Description des opérations de traitement envisagées et de leur(s) finalité(s) ;
- Evaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ;
- Evaluation des risques pour les droits et libertés des personnes concernées ;
- Identification et description des mesures envisagées pour faire face aux risques.

La CNIL met à disposition des responsables de traitements des lignes directrices pour les accompagner dans cette démarche.

Lorsque l'analyse d'impact révèle que le traitement représente un risque élevé en l'absence de mesures adéquates, le responsable du traitement doit soumettre le traitement envisagé à la consultation préalable de la CNIL.

d) Renforcement de l'obligation de sécurité

En parallèle des autres obligations mises à sa charge, le responsable du traitement voit également son obligation de sécurisation des traitements renforcée.

En effet, chaque responsable de traitement doit mettre en œuvre *« les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté »* (article 32).

Ces mesures peuvent notamment consister en :

- La pseudonymisation et le chiffrement des données ;
- Des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et des services de traitement ;
- Des moyens permettant de rétablir la disponibilité des données en cas d'incident physique ou technique ;
- Une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles destinées à assurer la sécurité du traitement.

L'ensemble des mesures prises dans ce cadre doit, évidemment, être documenté afin de pouvoir en justifier en cas de contrôle et de se conformer ainsi à l'obligation d'accountability.

Le renforcement de l'obligation de sécurité à la charge du responsable du traitement passe également par une plus grande transparence concernant les éventuelles failles de sécurité pouvant intervenir.
A cet égard, le Règlement impose au responsable du traitement de notifier à la CNIL toute violation de données à caractère personnel et ce **dans un délai maximum de 72 heures** après en avoir eu connaissance.

Cette notification doit contenir, à tout le moins, les quatre informations suivantes :

- Description de la nature de la violation ;
- Nom et coordonnées du délégué à la protection des données ou, à défaut, de la personne à contacter ;
- Description des conséquences probables de la violation de données à caractère personnel ;
- Description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel.

Le Responsable du traitement a également l'obligation d'informer les personnes concernées de la violation de leurs données.

Il est à noter que le sous-traitant est soumis à une obligation identique à l'égard du responsable du traitement.

e) Renforcement de l'obligation d'information

Outre les informations relatives à l'identité du responsable du traitement, la finalité du traitement des données, le caractère obligatoire ou facultatif des réponses, les droits d'accès, de rectification, d'interrogation et d'opposition, la durée de conservation et l'éventuel transfert de données vers un pays tiers, déjà exigées par la législation actuelle, il convient de fournir également aux personnes concernées par le traitement les informations suivantes :

- Les coordonnées du DPD ;
- L'existence du droit à l'oubli et à la portabilité des données ;
- Le cas échéant, l'existence du droit de retirer son consentement ;
- Le droit d'introduire une action devant une autorité de contrôle ;
- L'existence d'une prise de décision automatisée, y compris un profilage, et au moins en pareil cas, des informations utiles concernant la logique sous-jacente ainsi que l'importance et les conséquences prévues de ce traitement.

Lorsque les données personnelles traitées ne sont pas collectées auprès de la personne concernée, l'obligation d'information doit également mentionner la source d'où proviennent les données et le cas échéant, si elles sont ou non issues de sources accessibles au public.

3) Le Délégué à la Protection des Données

Le responsable du traitement et le sous-traitant doivent obligatoirement désigner un Délégué à la Protection des Données (DPD) dans les cas suivants :

- Le traitement est effectué par une autorité ou un organisme public ;
- Les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui exigent un suivi régulier et systématique à grande échelle des personnes concernées ;
- Les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de données sensibles ou relatives à des condamnations pénales et à des infractions.

En dehors de ces cas, le responsable du traitement et le sous-traitant restent libres de désigner ou non un DPD. Cette désignation est toutefois encouragée par le G29 (actuelle CEPD) car elle participe au respect du principe d'accountability.

Le DPD peut être un salarié du responsable du traitement (ou du sous-traitant) ou une personne extérieure. En effet, contrairement à la loi française, le Règlement ne limite pas la possibilité d'externaliser la fonction de DPD en fonction du nombre de personnes chargées de la mise en œuvre, ou, qui ont directement accès aux traitements.

Le DPD peut par ailleurs être désigné pour plusieurs organismes sous certaines conditions, notamment être facilement joignable à partir de chaque lieu d'établissement pour être en mesure de communiquer efficacement avec les personnes concernées et de coopérer avec l'autorité de contrôle.

La personne désignée comme DPD doit présenter les compétences requises pour cette fonction et posséder notamment des :

- Connaissances spécialisées du droit et des pratiques en matière de protection des données personnelles tant au niveau européen que national ;
- Connaissances de l'activité de l'entreprise ;
- Compétences informatiques.

Le DPD devient le véritable « chef d'orchestre » de la conformité en matière de protection de données au sein de son organisme. Dans ce cadre, il se voit confier les missions suivantes :

- Informer et conseiller le responsable du traitement sur les obligations applicables ;
- Contrôler le respect de l'ensemble des règles de protection des données ;
- Assister le responsable du traitement dans le cadre des analyses d'impact ;
- Vérifier l'exécution des analyses d'impact ;
- Coopérer avec la CNIL ;
- Faire office de point de contact pour la CNIL.

Du fait des fonctions qu'il occupe, le DPD dispose d'un statut particulier.

Il doit être associé de manière appropriée et en temps utile à toute question relative à la protection des données et rend compte directement au niveau le plus élevé de l'organisme pour lequel il intervient. Totalement indépendant dans le cadre de l'accomplissement de ses missions, il ne reçoit aucune instruction et n'est susceptible d'aucune sanction en raison de faits liés à sa mission.
En outre, étant amené à connaître des informations sensibles quant aux activités du responsable du traitement, le DPD est soumis au secret professionnel ou à une obligation de confidentialité.

Des lignes directrices ont été publiées par le G29 tant afin d'accompagner les responsables de traitement et les sous-traitants dans la mise en place de la fonction de délégué que d'assister ces délégués dans l'exercice de leurs missions.

Elles contiennent des recommandations et des bonnes pratiques permettant aux professionnels de se préparer et de mettre en œuvre leurs obligations avec flexibilité et pragmatisme.

4) Sous-traitance

Allant au-delà de la législation actuelle en la matière, le Règlement impose au responsable du traitement qui choisit de faire appel à un sous-traitant de vérifier que ce dernier présente *« **des garanties suffisantes** quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée »* (article 28).

Le responsable du traitement et le sous-traitant doivent, de surcroît, être liés par un contrat **écrit** dont le Règlement liste de manière non exhaustive le contenu (encadrement de la sous-traitance ultérieure, coopération avec le responsable de traitement dans la mise en œuvre des mesures de sécurité ou encore la réalisation de l'analyse d'impact, la mise à disposition d'informations pour que le responsable de traitement puisse procéder à des audits, etc.).
Le sous-traitant lui-même voit ses obligations alourdies tant à l'égard du responsable du traitement que des personnes concernées par le traitement.

Le sous-traitant ne peut plus se contenter de fournir des services sans connaître les traitements auxquels il prend part.

Il est tenu :

- d'une obligation de conseil à l'égard du responsable du traitement lui imposant notamment de l'informer s'il considère que l'une de ses instructions constitue une violation du Règlement ;
- d'une obligation d'assistance pour la mise en œuvre des obligations issues du Règlement notamment lors de la réalisation d'études d'impact.

Le sous-traitant, à l'instar du responsable du traitement, est par ailleurs astreint à une obligation de sécurité du traitement lui imposant la mise en œuvre de mesures techniques et organisationnelles appropriées.

Enfin, la responsabilité du sous-traitant peut directement être mise en cause en justice par les personnes concernées par le traitement si elles ont subi un dommage en raison d'une violation des dispositions du Règlement par le sous-traitant.

5) Transfert de données

Le responsable du traitement et/ou les sous–traitants peuvent transférer des données hors UE seulement s'ils encadrent ces transferts avec des outils assurant un niveau de protection suffisant et approprié des personnes.

Ainsi, et hormis les transferts fondés sur une décision d'adéquation de la Commission Européenne, les responsables de traitement et les sous-traitants peuvent mettre en place :

- Des règles d'entreprises contraignantes (BCR) ;

- Des clauses contractuelles types approuvées par la Commission Européenne ;
- Des clauses contractuelles adoptées par une autorité et approuvées par la Commission européenne (ex : privacy shield pour le transfert vers les Etats-Unis).

Par ailleurs, les données transférées hors Union restent soumises au droit de l'Union non seulement pour leur transfert, mais aussi pour tout traitement et transfert ultérieur.

6) Droit des personnes

Grâce aux nouvelles règles, les citoyens peuvent davantage contrôler leurs données personnelles.

a) Le renforcement du consentement

Les personnes concernées par le traitement doivent être informées dans un langage clair et précis de l'usage de leurs données et doivent en principe donner leur accord pour le traitement de leurs données, ou pouvoir s'y opposer.

La charge de la preuve du consentement incombe au responsable du traitement.

Le consentement doit être **clair et explicite** : l'individu doit donner son consentement de manière active ex : cocher une case lors de la visite d'un site Internet.

Le silence, des cases pré-cochées ou l'inactivité ne constituent donc pas un consentement.

Les personnes concernées pourront de plus retirer leur consentement à tout moment.

b) Le droit à l'oubli

Le droit à l'oubli permet aux personnes concernées de solliciter l'effacement de leurs données personnelles lorsqu'elles ne souhaitent plus que leurs données soient traitées, à condition qu'il n'existe aucune raison légitime de les conserver (ex : données nécessaires à des fins historiques, statistiques ou de recherche scientifique, pour des raisons de santé publique, ou pour l'exercice du droit à la liberté d'expression).

Dans l'hypothèse où ce droit est mis en œuvre, le responsable du traitement doit répercuter la demande à toute autre partie qui duplique les données concernées.

c) Le droit à la portabilité des données

Toute personne a le droit de récupérer les données qu'elle a fournies sous une forme aisément réutilisable, et, le cas échéant, de les transférer ensuite à un tiers.

Ce droit permet par exemple à un utilisateur de changer de fournisseur de messagerie électronique sans perdre ses contacts ou ses courriels.

d) Limitation du recours au profilage

Les dispositions fixent des limites au profilage, une technique utilisée pour analyser ou prédire les performances d'une personne au travail, sa situation économique, sa localisation, sa santé, ses préférences, sa fiabilité ou son comportement grâce au traitement automatique de ses données personnelles.

Conformément au Règlement, le profilage est, en règle générale, uniquement autorisé si la personne concernée donne son consentement, si la loi le permet et s'il est nécessaire à la conclusion d'un contrat.

Le profilage ne doit pas entraîner de discrimination ou se baser uniquement sur des données sensibles (telles que les données révélant, entre autres, l'origine ethnique, les opinions politiques, la religion, l'orientation sexuelle, les données génétiques ou biométriques, des sanctions administratives ou des suspicions) ni sur le traitement automatique des données.

Il doit comprendre une évaluation menée par l'homme, incluant une explication de la décision conclue après un tel examen.

e) Protection spéciale pour les enfants

Des garanties spéciales sont prévues pour les enfants, moins conscients des risques et conséquences liés au partage de leurs données personnelles.

Ils bénéficient ainsi d'un droit à l'oubli plus clair.

Par ailleurs, en dessous d'un certain âge, les enfants doivent avoir une autorisation parentale pour ouvrir un compte sur les réseaux sociaux, tels que Facebook, Instagram ou Snapchat, comme c'est déjà le cas dans la plupart des pays de l'UE. Il revient aux États membres de déterminer la limite d'âge qui doit être située entre 13 et 16 ans.

L'autorisation parentale n'est pas nécessaire pour utiliser des services de conseil ou de prévention directement destinés aux enfants.

7) Sanctions

a) Responsabilité directe

Le responsable du traitement ainsi que le sous-traitant sont directement responsables devant les personnes concernées du respect des dispositions du Règlement.

Ainsi, en cas de violation, toute personne peut au choix introduire une réclamation devant l'autorité de contrôle compétente ou saisir directement une juridiction pour solliciter la réparation du dommage qu'elle a subi du fait de cette violation.

La violation du Règlement par le responsable du traitement ou le sous-traitant peut également donner lieu à une action de groupe.

b) Sanctions administratives

Le responsable du traitement et le sous-traitant peuvent faire l'objet de sanctions administratives importantes en cas de méconnaissance des dispositions du Règlement.

Les autorités de protection peuvent notamment :

- Prononcer un avertissement ;
- Mettre en demeure le responsable du traitement ou le sous-traitant ;
- Limiter temporairement ou définitivement un traitement ;
- Suspendre les flux de données ;
- Ordonner de satisfaire aux demandes d'exercice des droits des personnes ;
- Ordonner la rectification, la limitation ou l'effacement des données ;
- Retirer la certification délivrée ou ordonner à l'organisme de certification de la retirer.

Des amendes administratives peuvent également être prononcées et représentent, selon la catégorie de l'infraction :

- 2% à 4% du chiffre d'affaires annuel mondial pour les entreprises ;
- 10 à 20 millions d'euros pour les autres organismes.

CONCLUSION

Afin de se mettre en conformité avec le RGPD, il est préconisé de suivre différentes étapes, détaillées ci-dessous.

Tout d'abord, il convient de désigner un groupe de travail ou un référent dans l'entreprise, chargé de la gestion de ces questions relatives aux données personnelles.
Nonobstant la désignation de ces personnes, tout le personnel de l'entreprise, doit être sensibilisé à cette nouvelle réglementation.

Ensuite, un état des lieux de l'existant est à mettre en place. Il s'agit ici de s'assurer de la conformité de ses sites internet (mentions légales, cookies, demande de consentement lors de la collecte des données, information des personnes sur leurs droits) et de faire l'inventaire de tous les traitements de

données personnelles mis en place dans l'entreprise. Ainsi, il faut recenser, au sein de chaque service, les différentes données collectées, identifier les modalités de leur collecte, leur localisation et leur lieu de stockage et lister l'intégralité de ces informations.
Cet inventaire doit permettre de déterminer notamment la base légale du traitement (consentement, exécution du contrat, obligation légale ou intérêt légitime), la finalité de ce dernier, le destinataire des données (sous-traitant, transfert dans l'UE ou hors UE) et leur durée de conservation.

Une cartographie des flux peut alors être entreprise. Il revient alors à l'entreprise d'analyser toute sa documentation, aussi bien interne (règlement intérieur, charte, notes de service, déclarations/autorisations faites préalablement auprès de la CNIL, contrats de travail et de sous-traitance…), qu'externe en vérifiant les documents mis à disposition des clients (cartes de fidélité, jeux concours, conditions générales de vente, …).

Il faut vérifier également son système de sécurisation informatique, en identifiant les moyens et procédures de la sécurité informatique utilisés tant physiques (la sécurité physique des locaux) que logiques.

Une fois toutes ces informations recueillies, on peut établir un rapport.

Après avoir listé les différents traitements effectués, il convient d'identifier les risques qui y sont associés. Il peut s'agir de menaces relatives à la confidentialité (en cas de vol de dossier ou de support ordinateur/clé USB…), à l'intégrité (suppression des données par erreur ou ajout de matériel incompatible entrainant la perte des données…) ou encore à la disponibilité (en cas de perte d'un dossier lors du déménagement de l'entreprise ou en cas de rachat…).

Au regard des écarts soulevés avec la réglementation, il est possible de répondre par des mesures techniques (sécurisation du matériel , des locaux, chiffrement, …), juridiques (pseudonymisation, minimalisation de la collecte, information des salariés et des clients sur les traitements, détermination d'une durée de traitement, formation et sensibilisation du personnel, clause dans le contrat de sous-traitance,…) mais aussi organisationnelles (tenue d'un registre des traitements, documentation des mesures de protection, notification en cas de violation de données,…).
Il peut être nécessaire de mener une étude d'impact en cas de risque pour les droits et libertés des personnes. Si un risque élevé est identifié, l'étude d'impact est obligatoire (également obligatoire dans 3 cas listés à l'article 35 du règlement 2016/679). En revanche, il n'est pas nécessaire d'effectuer une telle étude dans l'hypothèse où l'entreprise considère qu'il n'existe pas de risque lié au traitement (article 35§1, 3 et 4 du RGPD). Mais elle devra justifier de son choix. La CNIL a dispensé certains types d'opérations de l'analyse d'impact en publiant des listes des traitements concernés et des traitements non concernés : https://www.cnil.fr/fr/analyse-dimpact-relative-la-protection-des-donnees-publication-dune-liste-des-traitements-pour et https://www.cnil.fr/fr/liste-traitements-aipd-non-requise

Enfin, dans certains cas, la désignation d'un délégué à la protection des données (DPD) est imposée (article 37 du RGPD). En dehors des 3 cas prévus, la désignation d'un DPD par le responsable de

traitement est facultative mais recommandée car elle permet d'assurer la mise en œuvre du règlement. En cas de désignation d'un DPD, il convient d'en informer la CNIL et les salariés. Dans l'hypothèse inverse, le responsable de traitement doit justifier son choix de ne pas désigner de DPD.

En tout état de cause, l'entreprise sera bien inspirée d'anticiper un contrôle en mettant en place une procédure interne prévoyant les modalités à mettre en œuvre dans une telle hypothèse (personne référente, vérification du périmètre d'intervention…) afin de ne pas se faire surprendre par un contrôle inopiné.
Enfin, c'est probablement pour l'entreprise le moment de vérifier ses polices d'assurances et de les complémenter d'une assurance cyber sécurité.

8) Sources et liens utiles :

- Règlement (UE) 2016/679 :
https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679

- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés :
https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460&dateTexte=20190218

- Q&R : législation européenne sur la protection des données :
http://www.europarl.europa.eu/news/fr/news-room/20160413BKG22980/nouvelle-l%C3%A9gislation-europ%C3%A9enne-sur-la-protection-des-donn%C3%A9es

- Règles relatives à la protection des données à caractère personnel au sein et à l'extérieur de l'UE :
https://ec.europa.eu/info/law/law-topic/data-protection_fr

- Lignes directrices concernant les délégués à la protection des données (DPD) :
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf

(Pour une version dans les autres langues européennes :
http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48137)

- Le règlement général sur la protection des données - RGPD (CNIL) :
https://www.cnil.fr/fr/reglement-europeen-protection-donnees/

- Comprendre le RGPD : Ce qui change pour les professionnels :
https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels

- Analyse d'impact sur la vie privée : guides, outil, « PIAF », étude de cas : https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-aipd

Benjamin May - Clémentine Richard *« Données personnelles ce qui va concrètement changer pour les entreprises »*, Expertise Juillet/Août 2016

La CNIL publie son registre RGPD : https://www.cnil.fr/fr/la-cnil-publie-son-registre-rgpd

Registre des activités de la CNIL : https://www.cnil.fr/sites/default/files/atoms/files/registre-rgpd-cnil_mai-2020.pdf

Guide d'autoévaluation de maturité en gestion de la protection des données pour les entreprises : https://www.cnil.fr/fr/la-cnil-propose-une-autoevaluation-de-maturite-en-gestion-de-la-protection-des-donnees